

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-191459

(43) 公開日 平成10年(1998) 7月21日

(51) Int.Cl.<sup>6</sup>

識別記号

F I

H 0 4 Q 7/38

H 0 4 B 7/26

1 0 9 R

H 0 4 L 9/30

H 0 4 L 9/00

6 6 3 A

6 6 3 B

審査請求 未請求 請求項の数11 O L (全 10 頁)

(21) 出願番号 特願平9-304553

(22) 出願日 平成9年(1997)11月6日

(31) 優先権主張番号 08/744682

(32) 優先日 1996年11月6日

(33) 優先権主張国 米国 (U S)

(71) 出願人 590005612

ノキア モービル フォーンズ リミティ  
ド

フィンランド国, エフアイエヌ-02150  
エスポー, ケイララーデンティエ 4

(72) 発明者 ティエ ルオ

アメリカ合衆国, テキサス 76006, アー  
リントン, サンライト ドライブ 2606

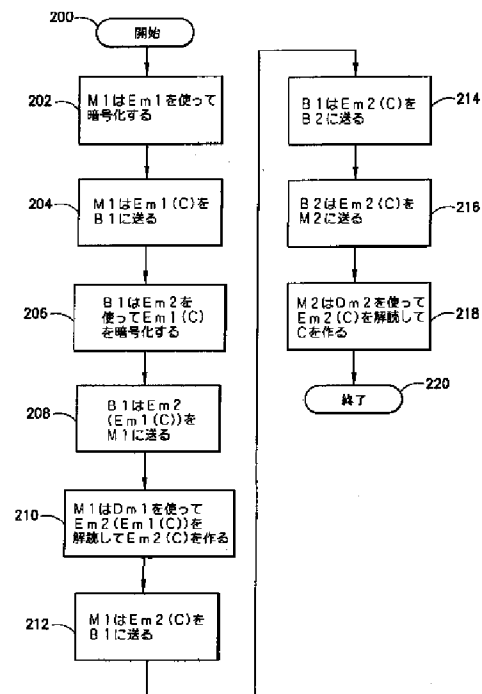
(74) 代理人 弁理士 石田 敬 (外3名)

(54) 【発明の名称】 通信システムにおいて機密保護メッセージを送る方法

(57) 【要約】

【課題】 公開の暗号化キーを用いて機密保護メッセージを送る。

【解決手段】 送信側は自分の公開の暗号化キーExを使ってメッセージcを暗号化し、その暗号化されたメッセージEx(c)を受信側に送る。受信側は、そのメッセージの目的の受取手の暗号化キーEyを使って暗号化メッセージEx(c)を暗号化してメッセージEy(Ex(c))を作り、このメッセージEy(Ex(c))を送信側に送る。送信側は自分の秘密の解読キーを使ってそのメッセージEy(Ex(c))を解読してDx(Ey(Ex(c)))=Ey(c)を作り、このメッセージEy(c)を受信側に送る。受信側は、自分がそのメッセージの目的の受取手であるならば、自分自身の解読キーDyを使ってそのメッセージを解読してDy(Ey(c))=cを作り、自分がそのメッセージの目的の受取手ではなければ、受取手に送り、受取手が自分自身の解読キーDyを使ってそのメッセージを解読する。



## 【特許請求の範囲】

【請求項1】 少なくとも1つの基地局と複数の移動局とを有する通信システムで機密保護メッセージを送る方法において、前記方法は：各移動局に解読キーと公開の暗号化キーとを割り当て；第1移動局において前記第1移動局の暗号化キーを用いて第1メッセージを暗号化して第2メッセージを作り；前記第2メッセージを前記第1移動局から前記の少なくとも1つの基地局に送り；前記の少なくとも1つの基地局において第2移動局の暗号化キーを用いて前記第2メッセージを暗号化して第3メ  
10 ヌッセージを作り；前記第3メッセージを前記の少なくとも1つの基地局から前記第1移動局に送り；前記第1移動局において前記第1移動局の解読キーを用いて前記第3メッセージを解読して第4メッセージを作り；前記第4メッセージを前記第1移動局から前記の少なくとも1つの基地局に送り；前記第4メッセージを前記の少なくとも1つの基地局から前記第2移動局に送り；前記第2移動局において前記第2移動局の解読キーを用いて前記第4メッセージを解読して前記第1メッセージを作り直すステップから成ることを特徴とする方法。

【請求項2】 前記第1移動局の解読キー及び暗号化キー、並びに前記第2移動局の解読キー及び暗号化キーは、前記第2移動局の暗号化キーをメッセージに適用して第1結果を得てから前記第1移動局の解読キーをその第1結果に適用して最終結果を得ることが、前記第1移動局の解読キーを前記メッセージに適用して第2結果を得てから前記第2移動局の暗号化キーを前記第2結果に適用して前記最終結果を得ることと同等であるように構成されていることを特徴とする請求項1に記載の方法。

【請求項3】 前記第1移動局において暗号化及び解読を行う前記ステップは第1アルゴリズムに従って行われ、前記第2移動局において暗号化及び解読を行う前記ステップは第2アルゴリズムに従って行われることを特徴とする請求項1に記載の方法。

【請求項4】 前記第1アルゴリズムはRSA型のアルゴリズムから成り、前記第2アルゴリズムはラビン型のアルゴリズムから成ることを特徴とする請求項3に記載の方法。

【請求項5】 前記第1アルゴリズムはラビン型のアルゴリズムから成り、前記第2アルゴリズムはRSA型のアルゴリズムから成ることを特徴とする請求項3に記載の方法。

【請求項6】 第1及び第2の送受信装置を有する通信システムで機密保護メッセージを送る方法において、前記方法は：前記の第1及び第2の送受信装置の各々に解読キー及び公開の暗号化キーを割り当て；前記第1送受信装置において前記第1送受信装置の暗号化キーを用いて第1メッセージを暗号化して第2メッセージを作り；前記第2メッセージを前記第1送受信装置から前記第2送受信装置に送り；前記第2送受信装置において前記第  
50

2送受信装置の暗号化キーを用いて前記第2メッセージを暗号化して第3メッセージを作り；前記第3メッセージを前記第2送受信装置から前記第1送受信装置に送り；前記第1送受信装置において前記第1送受信装置の解読キーを用いて前記第3メッセージを解読して第4メッセージを作り；前記第4メッセージを前記第1送受信装置から前記第2送受信装置に送り；前記第2送受信装置において前記第4メッセージを解読して前記第1メッセージを作り直すステップから成ることを特徴とする方法。

【請求項7】 前記第1送受信装置の解読キー及び暗号化キー、並びに前記第2送受信装置の解読キー及び暗号化キーは、前記第2送受信装置の暗号化キーをメッセージに適用して第1結果を得てから前記第1送受信装置の解読キーをその第1結果に適用して最終結果を得ることが、前記第1送受信装置の解読キーを前記メッセージに適用して第2結果を得てから前記第2送受信装置の暗号化キーを前記第2結果に適用して前記最終結果を得ることと同等であるように構成されていることを特徴とする請求項6に記載の方法。

【請求項8】 前記第1送受信装置において暗号化及び解読を行う前記ステップは第1アルゴリズムに従って行われ、前記第2送受信装置において暗号化及び解読を行う前記ステップは第2アルゴリズムに従って行われることを特徴とする請求項6に記載の方法。

【請求項9】 前記第1アルゴリズムはRSA型のアルゴリズムから成り、前記第2アルゴリズムはラビン型のアルゴリズムから成ることを特徴とする請求項8に記載の方法。

【請求項10】 前記第1アルゴリズムはラビン型のアルゴリズムから成り、前記第2アルゴリズムはRSA型のアルゴリズムから成ることを特徴とする請求項8に記載の方法。

【請求項11】 前記第2送受信装置は第1基地局から成り、前記第1送受信装置は第1移動局から成り、前記通信システムは更に第2基地局と第2移動局とを有し、前記方法は更に：前記第1メッセージを前記第1基地局から前記第2基地局に送り；前記第2基地局において前記第2基地局の解読キーを用いて前記第1メッセージを暗号化して第5メッセージを作り；前記第5メッセージを前記第2基地局から前記第2移動局に送り；前記第2移動局において前記第2移動局の暗号化キーを用いて前記第5メッセージを暗号化して第6メッセージを作り；前記第6メッセージを前記第2移動局から前記第2基地局に送り；前記第2基地局において前記第2基地局の解読キーを用いて前記第6メッセージを解読して第7メッセージを作り；前記第7メッセージを前記第2基地局から前記第2移動局に送り；前記第2移動局において前記第2移動局の解読キーを用いて前記第7メッセージを解読して前記第1メッセージを作り直すステップを有する

ことを特徴とする請求項6に記載の方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、通信システムのための暗号化技術に関し、特に通信システムにおいて公開の暗号化キーを使用して機密保護メッセージを送る装置及び方法に関する。

【0002】

【従来の技術】通信システム技術が進歩して、いろいろな通信システム及びサービスを利用できるようになっている。それらのシステムの中には、セルラー電話通信網、個人通信システム、種々のページングシステム、及び種々の有線及び無線のデータ通信網が含まれる。今日アメリカ合衆国で使用されているセルラー電話通信網は、AMPSアナログシステム、デジタルIS-136時分割多重(TDMA)システム、及びデジタルIS-95デジタル符号分割多重(CDMA)システムを含む。ヨーロッパでは、移動通信用広域(GSM)デジタルシステムが最も広く使用されている。これらのセルラーシステムは800-900MHzの範囲で動作する。個人通信システム(PCS)も合衆国で現在展開されている。多くのPCSシステムが1800-1900MHz範囲に対して開発されつつあるが、それらは各々主要なセルラー規格のうちの1つに基づいている。

【0003】上記の通信システムの各々において、該システムのオペレータがシステムのユーザーに機密保護通信手段を提供することが望ましいことがしばしばある。それは、該システムで動作している2つの移動局の間で機密保護メッセージを送ることを含むことがある。多くの場合にそのメッセージはテキストメッセージ等の、有

限の長さのテキストメッセージである。

【0004】AMPS等のアナログシステムでは、通信内容を機密保護するのは非常に難しい。2ユーザー間で通信内容を運ぶ信号がアナログの性質であるために暗号化を簡単に効率的にも行うことはできない。実際、標準的AMPSでは、暗号化は全く行われず、移動局と基地局との間で送られる通信メッセージは監視されたり傍受されたりされ得る。通信チャンネルに使用される周波数に同調させることのできる受信装置を持っているものは誰でも、見つかることなく何時でも通信を傍受することができる。この傍受の可能性は、AMPS等のアナログシステムに結びついた1つの不都合な要素であった。この様に傍受される可能性があるために、AMPS型のシステムは機密保護メッセージを送ることを必要とする或る種のビジネスユーザーや政府筋のユーザーには好まれていない。

【0005】通信の秘密を目的として暗号化サービスを含むGSM、IS-136及びIS-95等の新しいデジタルシステムが開発されている。これらのデジタルシステムで2ユーザー間で通信メッセージを運ぶ音声信号

或いはデータ信号はデジタルの性質を持っているので、ランダム或いは疑似ランダムの性質を持っている通信信号を作るための暗号化装置を通して処理され、認可された受信装置で解読される。このようなシステムで機密保護メッセージを送りたいときには、該システムの暗号化機能を使ってメッセージを暗号化することができる。例えば、これらの規格で指定されているショートメッセージサービス(SMS)機能を使って、該システムの暗号化アルゴリズムに従って暗号化されているテキストメッセージを送ることができる。

【0006】GSM、IS-136、及びIS-95システムでは、暗号化は各ユーザーとシステムとの間のメッセージ送信に対して秘密のキー値“非公開キー”を用いて行われ、そのキーはシステムと通信するユーザーとシステムとだけに知られている。ここで検討しているPCS通信網についてのシステム規格は、特定のPCS規格の淵源となるデジタル規格、即ちGSM、IS-136、或いはIS-95において指定されている暗号化技術に基づく暗号化サービスを包含することもできる。

【0007】GSMではシステムのオペレータがシステムの各ユーザーに加入者識別モジュール(SIM)を発行することによって機密保護プロセスを制御する。SIMは、ユーザーが呼を発したり受けたりするのに使う移動局に挿入しなければならない差し込み式のチップ又はカードである。SIMは、各ユーザーに独特の、Kiと呼ばれる128ビットの数を内蔵している。このKiは、確認と、暗号化キーの導出との両方のために使われる。GSMでは、各ユーザーを確認してそのユーザーについてのKiから暗号化ビットを作成するために呼びかけと応答の手続が使われる。この呼びかけと応答の手続をホームシステムの自由裁量で実行することができる。

【0008】GSM移動局が自分のホームシステムで動作しているとき、ユーザーが自分の国際移動システム識別子/一時移動システム識別子(international mobile system identity/temporary mobile system identities (IMSI/TMSI))を呈示することによって自分が誰であるかを明らかにした後、該システムで128ビットの乱数(RAND)が作成されてその移動局のユーザーのKiと結合されて32ビットの応答(SRES)となる。このときシステムはRANDを該移動局に送り、該移動局はそのユーザーのKiから自分自身のSRES値を計算し、このRANDをシステムに送り戻す。もしその2つのSRESが調和するならば、その移動局は本物であると判断される。暗号化キー“Kc”を作るために、該移動局及び通信網の両方においてRAND及びKiを使用するアルゴリズムにより、該移動局とシステムとの間の通信のための暗号化ビットが作成される。その後、Kcは両端で機密保護通信を行うために使用される。GSM移動局が移動中であるとき、該移動局が訪れたシステムにおいて該ユーザーの登録が行われるときに、或いは

ユーザーが訪れたシステムから特別の要求が行われたときに、そのシステムにRAND、SRES及びKcの値が転送される。Ki値はホームシステム及びユーザーのSIM以外では決して使用し得ない。

【0009】IS-136及びIS-95の確認及び暗号化の処理手順は互いに同一であり、またGSMの確認及び暗号化の処理手順と似ている。IS-136システム及びIS-95システムでは、呼びかけと応答の方法も利用される。そのIS-136及びIS-95の方法は、“Aキー”と呼ばれる機密保護キーを利用する。各移動局についての64ビットのAキーはシステムのオペレータによって決定される。各移動局についてのAキーはその移動局の所有者のホームシステムとその移動局自体とに記憶される。最初にAキーは米国郵便等の安全な方法で移動局の所有者に通知され得る。その所有者はキーパッドを介してそのAキーを移動局に入力することができる。或いは、Aキーを工場或いは点検修理の場所で移動局にプログラムすることもできる。Aキーは、移動局及びホームシムの両方で共有される秘密データ（shared secret data (SSD)）を所定のアルゴリズムから作成するために使われる。各移動局についてのSSDは、ホームシステムのオペレータのみが開始することのできるオーバーエア・プロトコル（an over the air protocol）の使用によってその移動局のAキーから定期的に導出され更新され得る。

【0010】IS-136及びIS-95の確認及び暗号化では、32ビットの広域呼び掛けが該移動局のサービスエリアのシステム内で所定間隔をおいて作成されて放送される。移動局がホームシステムにおいてシステム登録／呼設定アクセスを試みると、該移動局においてそのSSDから18ビットの確認応答を計算するために現在の広域呼び掛け応答が使用される。その後、その確認応答とその移動局についての呼カウント値を含むアクセス要求メッセージが該移動局からホームシステムに送られる。そのアクセス要求を受け取ると、ホームシステムは広域呼び掛け及びその移動局のSSDを使ってそれ自身の応答値を計算する。確認応答と、その移動局のSSDと、呼カウント値を含む他の関連データとの比較によって、その移動局が本物であると確認されれば、その移動局は登録される。

【0011】移動局が訪問先のシステムでシステム登録／呼設定アクセスを試みると、現在の広域呼び掛け応答を用いて該移動局において該移動局のSSDから18ビットの確認応答を計算する。次にアクセス要求メッセージが該移動局から訪問先のシステムに送られる。訪問先のシステムでの初期登録アクセスについては、アクセス要求メッセージは移動局で計算された確認応答を含む。確認応答と広域呼び掛けとは該移動局のホームシステムに送られ、該ホームシステムはその広域呼び掛けと該移動局のSSDとを使ってそれ自身の応答値を計算す

る。確認応答同士を比較することによってその移動局が本物であると確認されたならば、その移動局のSSDと、呼カウント値を含む他の関連データとが訪問先のシステムに送られて該移動局が登録される。該移動局が関わる呼が設定されるとき、現在の確認応答値と呼カウントとが該移動局から呼設定情報とともに該システムに送られる。呼設定情報を受け取ると、訪問先のシステムは、要求をしている移動局についての記憶されているSSDと呼カウント値とを検索する。その後、訪問先のシステムは、受け取ったSSD値と現在の広域呼び掛けとが該移動局で作られたのと同じ応答を作ること確かめるために確認応答値を計算する。もしその確認応答同士と呼カウント同士とが揃うならば、その移動局は呼アクセスを許可される。通信の機密保護が希望される場合には、暗号化キー・ビットを作成するために広域呼び掛けと該移動局のSSDとを入力として用いて暗号化キーが該移動局とシステムとの両方で作成される。

【0012】GSM、IS-136及びIS-95システムで使用されるような技術についての更なる背景情報が“IEEE個人通信”の6-10頁の1995年8月付けのダン・ブラウンによる“個人通信システムにおけるプライバシー及び確認のための技術”という論文（the article “Techniques for Privacy and Authentication in Personal Communications Systems” by Dan Brown in IEEE Personal Communications, dated August 1995, at pages 6-10）に開示されている。

【0013】GSM、IS-136及びIS-95システムで使用される上記の機密キー処理手順は通信の機密を保護するものであるけれども、これらの処理手順のいずれも、傍受及び盗聴を完全に免れ得るわけではない。これらの処理手順の全てが、ユーザーのAキー又はKi値が移動局とホームシステムとの双方に知られていることを必要とする。これらの処理手順は、ユーザーのSSD又はKc値が通信リンクの両端即ちシステム及び移動局の双方において知られていることをも必要とする。これらの各値がもしかすると改悪されて傍受者に知られてしまっているという可能性もあり得る。ユーザーのKi又はAキーを知っている人、或いはシステム間通信をしているユーザーのKc又はSSDを傍受した人は、機密保護されるべき通信を傍受し盗聴する可能性がある。また、各ユーザーのキーは、該ユーザーが通信をする基地局で利用可能であるので、システムの基地局を通して接続している2つの移動局が関わる暗号化通信がその基地局で破られる可能性がある。

【0014】公開キー暗号化方法は、ユーザーに公開の、即ち公然と知られ明らかにされるかも知れない暗号化キーが割り当てられるけれども、またそのユーザーにしか知られない秘密の解読キーもユーザーに割り当てられるようになっている方法である。目的の受信側ユーザーの解読キーだけがそのユーザーに宛てられた暗号化さ

れたメッセージを解読することができる、即ちその目的の受信側ユーザーの暗号化キーを使って暗号化されたメッセージを解読することができる。公開キー暗号化通信システムでは、ユーザーは解読キーを基地局やシステムから隠して自分で保管しておくことを許されるであろう。メッセージを解読するのに必要なキーを知っているのは受信側のユーザーだけであるので、公開キー暗号化方法は、例えばGSM、IS-136、或いはIS-95で使われている現在の暗号化技術で得られるよりも一層安全な通信を提供することができる。

【0015】在来の公開キー暗号化方法を使用するセルラーシステムでは、移動局Xが暗号化されたメッセージを移動局Yに送るとすると、移動局Xは、移動局Yのための公開暗号化キーと、移動局Yの暗号化キーとともに使用されなければならないアルゴリズムとの両方を知る必要がある。移動局Xが移動局Yの暗号化キーとアルゴリズムとを使ってメッセージを暗号化することができることも必要であろう。在来の公開キー暗号化方法のこれらの要件は、場合によってはセルラーシステムで使用するに当たって或る種の困難を引き起こしたり、或いは余り適していないかも知れない。

【0016】

【発明が解決しようとする課題】公開キー暗号化法を使用するに当たっての1つの難点は、暗号化と解読とに必要な計算が秘密キーシステムで必要とされるよりも遥かに多量の計算資源を必要とするかも知れないことである。移動局ではその様な計算資源には限りがあるかも知れない。二人の移動局ユーザーが各々異なる暗号化／解読アルゴリズムを使ってメッセージを秘密裏に交換したいと望む場合には資源に関する要件はもっと大きくなり得る。例えば、移動中の移動局のホームシステムのアルゴリズムとは異なる自分独自のアルゴリズムを実行するための手段をシステムオペレータが備えているシステムにその移動中の移動局が入り込んだときなどには、前記のように資源に関する要件が大きくなるかも知れない。この場合、どの移動局も、他のユーザーのアルゴリズムで暗号化を行うとともにその移動局のユーザーのアルゴリズムで解読を行うことができなければならないであろう。例えば、暗号化するために使われるアルゴリズムが、その暗号化を実行する移動局で利用し得るよりも多量の計算資源を必要とするならば、その様な要件を満たすのは困難であるかも知れない。また、特定のアルゴリズムを実行するためのコード及びデータを各移動局に記憶させておくか或いは暗号化開始前に該移動局に送信しなければならないであろうから、移動局の計算資源に対する要求が更に大きくなる。

【0017】セルラーシステムで公開キー暗号化法を使用することについてのもう一つの潜在的難点は、メッセージを送信側移動局或いは受信側移動局だけが利用し得ることを保証するために送信側の移動局が受信側移動局

の暗号化キーを知っていなければならないということである。或る種の公開キー暗号化法では暗号化キーは各々非常に大きい可能性があり、それは場合によっては数列であり、受信側となる可能性のある全ての移動局のための暗号化キーを1つの移動局に記憶させるのは困難であるかも知れない。受信側の移動局のキーがもし非常に大きければ、例えば呼設定時などに、必要に応じて送信側移動局に送ることも困難であるかも知れない。

【0018】

10 【課題を解決するための手段】本発明は、公開キー暗号化法を使用する通信システムにおいて機密保護メッセージを送る方法を提供する。この方法は、ユーザーの解読キーがそのユーザーの送受信装置においてのみ知られることとなるように実施される。この方法は、ユーザーの送受信装置がそのユーザーの暗号化／解読アルゴリズムと暗号化キーとを使用できるだけでよいようにも実施される。これは、特別のシーケンスを用いて2つの送受信装置間でメッセージを交換することにより実行される。この方法は、機密キー法の使用に伴う機密保護問題を回避し、各移動局がそれ自身の公開キー暗号化／解読アルゴリズムのみを実行できるようにする。この方法では、

20 在来の公開キー暗号化法の場合のように送受信装置が目的の受信側送受信装置の暗号化キーとアルゴリズムとを使って暗号化を実行できることを必要としない。従って、送受信装置の計算資源を特定の1つのアルゴリズム向けに最適化することができる。

【0019】この方法は、各移動局或いは通信網が各々異なる暗号化／解読アルゴリズムを使用する2つの移動局間又は移動局及びセルラー通信網の間で機密保護メッセージが交換されるときに非常に安全なショートメッセージサービス(SMS)テレサービスを提供するのに役立つ。この方法は、計算量の比較的に少ない機密キーアルゴリズムを使って音声伝送などの比較的に長い通信を行えるように、通信を行う2つの移動局間で或いは移動局と通信網との間で機密キーを交換するのに役立つ。また、1つの移動局から他の移動局又は通信網へ機密保護確認符号定数(a secure authentication signature)を送るためにこの方法を使用することもできる。

40 【0020】本発明の或る実施例では、2つのユーザー間で交換されるメッセージのポイント間暗号化法が少なくとも1つの基地局と複数の移動局とを有する通信システムで実施される。このポイント間実施例では、該システムの基地局では解読は行われない。移動局M1のユーザーには、公然と知られる(システムに知られる)暗号化キーEm1と移動局M1においてのみ知られる解読キーDm1とが割り当てられる(“暗号化キーEmx”及び“解読キーDmx”という用語は、ここではアルゴリズムとそのアルゴリズムで使用されるキー値との両方を指す、即ちEmxは暗号化キー値を使用する暗号化／解読アルゴリズムであり、Dmxは解読キー値を使用する

暗号化／解読アルゴリズムである)。移動局M2の他のシステムユーザーには、公然と知られる暗号化キーEm2と、移動局M2においてのみ知られる解読キーDm2とが割り当てられ、ここでDm1Em2=Em2Dm1である。Dm1Em2=Em2Dm1は、始めにDm1をメッセージに適用し次にEm2を適用するということとは始めにEm2を次にDm1をメッセージに適用することと同じであるという制限を課すものである。M1のみがDm1を知っており、M2のみがDm2を知っている。また、M1はEm1とM1の特別な暗号化／解読アルゴリズム(A1)とを知っているだけで良く、M2はEm2とM2の特別な暗号化アルゴリズム(A2)とを知っているだけで良い。

【0021】移動局M1を持っているユーザーが移動局M2のユーザーに機密保護通信メッセージcを送りたいとき、その通信メッセージcはM1においてEm1及びA1を用いて暗号化されてメッセージEm1(c)となる。M1はこのEm1(c)をシステムの基地局B1に送る。基地局B1はEm2とA2とを用いてEm1(c)を暗号化してメッセージEm2(Em1(c))を作成し、それをM1に送り戻す。次にEm2(Em1(c))はM1においてDm1及びA1を用いて解読される。Dm1Em2=Em2Dm1であるので、Dm1を用いてEm2(Em1(c))を解読するとEm2(c)が得られる。M1はEm2(c)をB1に送る。B1は、移動局M2が存在している区域を管理する基地局B2にEm2(c)を送る。次にEm2(c)は移動局M2に送られて移動局M2によってDm2及びA2で解読されて、移動局M1から移動局M2に送られた通信メッセージcと成る。

【0022】本発明の他の実施例では、2つの移動局間での非ポイント間暗号化法が通信システムで実施される。移動局M1のシステムユーザーには、公然と知られる(システムに知られる)暗号化キーEm1と、移動局M1においてのみ知られる解読キーDm1とが割り当てられる。M1は暗号化／解読アルゴリズムA1を使用する。移動局M2の他のシステムユーザーには、公然と知られる暗号化キーEm2と、移動局M2においてのみ知られる解読キーDm2とが割り当てられる。M2は暗号化／解読アルゴリズムA2を使用する。また、システムの各基地局Bxには、公然と知られる暗号化キーEb xと基地局Bxのみが知る解読キーDb xとが割り当てられる。各基地局はアルゴリズムAb xに従って暗号化／解読を行う。キーは、互いに通信する基地局Bxと移動局Mxとのいずれの対についてもDm xEb x=Eb xDm xとなるように選択される。

【0023】この実施例では、移動局M1を持っているユーザーが機密保護通信メッセージcを移動局M2のユーザーに送ることを望んでいるとき、通信メッセージcはM1でEm1及びA1を用いて暗号化されてメッセー

ジEm1(c)となる。M1はこのEm1(c)をシステムの基地局B1に送る。基地局B1はEb1及びAb1を用いてEm1(c)を暗号化してメッセージEb1(Em1(c))を作り、それをM1に送る。Eb1(Em1(c))は次にM1においてDm1及びAm1を用いて解読される。Dm1Eb2=Eb2Dm1であるので、Dm1を用いてEb1(Em1(c))を解読するとEb1(c)が得られる。次にM1はEb1(c)をB1に送る。B1は、Db1及びAb1を用いてEb1(c)を解読してcを作り、移動局M2が位置している地域を管理する基地局B2にcを送る。次にB2とM2との間で通信メッセージcはM1とB1との間での転送について述べたのと全く同様に暗号化されるが、この場合、B2、Eb2、Db2及びAb2がM1、Em1、Dm1及びAm1に代わり、M2、Em2、Dm2及びAm2がB1、Eb1、Db1及びAb1に代わる。

【0024】以下の詳細な説明を添付図面と関連させて読めば本発明の方法を一層充分に理解できる。

【0025】

【発明の実施の形態】図1は本発明の実施例に従って構成された通信システム100のブロック図である。システム100は、基地局B1及びB2、陸線通信網142、及び移動局M1及びM2から成る。2つの基地局と2つの移動局とを包含するものとして図示されているけれども、システム100は図1に示されているより多数或いは少数の基地局或いは移動局から成っていてもよい。移動局M1及びM2は、M1又はM2のユーザーと他の移動電話との間、或いはユーザーと陸線通信網142に接続された陸線電話との間で音声通信を提供する移動電話であってもよい。移動局M1及びM2は、個人通信装置或いは無線モデムを通して動作するラップトップ型コンピュータなどの、システム100についてのシステム規格に従って動作することのできる他の随意的種類の移动通信装置であってもよい。陸線通信網142は、公衆交換電話回線網(PSTN)、或いは、呼経路選択、登録、及びシステム100内での移動局の1つの基地局から他の基地局へのハンドオフを制御するための移動交換センターを包含するシステム100のための私設陸線通信網であってもよい。システム100では、移動局M1及びM2はRFリンクを通してシステム100の基地局と通信しながらシステム100の通達範囲の中を動き回ることができる。図1では、移動局M1及びM2は、それぞれRFリンク144及び146を介して基地局B1及びB2とそれぞれ通信しているものとして示されている。システム100は、RFリンクを介して移動局M1及びM2と基地局B1及びB2との間にデジタルインターフェースを提供する如何なる通信システム規格に従って動作してもよい。デジタル通信システムの設計及び動作は公知であるので、ここでは詳しくは説明しな

い。システム100はいろいろな方法で具体化され得る。例えば、システム100のデジタルRFインターフェースは、通信産業協会／電子産業協会（Telecommunications Industry Association/Electronic Industry Association (TIE/EIA)）のIS-136、IS-95、及びPCS1900規格或いはGSM規格に類似する規格に従って動作することができる。

【0026】移動局M1は、システム100の基地局と無線信号をやりとりするためのアンテナ102に結合されたトランシーバ・ユニット104を包含している。移動局M1はユーザーインターフェース108を包含しているが、それはコンピュータ・キーボードであるか、或いはキーパッド、マイクロホン及び受話口の付いている移動電話の送受器であり得る。移動局M1の制御ユニット106は、RFチャネル選択及びその他のシステム機能を通常の方法で制御し、論理ユニット112は該移動局の全般的動作を制御する。通信の機密保護を行うために使われる暗号化及び解読の機能を実現し実行するためにも論理ユニット112を利用することができる。ディスプレイ110は、移動局M1のユーザーに総合的視覚インターフェースを提供するものであり、論理ユニット112により制御される。移動局M2はトランシーバ・ユニット116、ユーザーインターフェース120、制御ユニット118、論理ユニット124、及びディスプレイ122を包含しており、これらは各々移動局M1の対応するセクションについて記載したのと同じ機能を持っている。

【0027】基地局B1は移動局と無線信号をやりとりするためのアンテナ134に結合されたトランシーバ・ユニット136を包含している。B1は制御ユニット138及び処理装置140も包含している。制御ユニット138は、移動局への適当な制御メッセージを作成することによってRFチャネル選択及び割り当てを制御するとともに、陸線通信網142とのインターフェーシングなどの他の所要のシステム機能も制御する。通信の機密保護のために使われる暗号化及び解読の機能を実現し実行するために処理装置140を利用することができる。基地局B2はトランシーバ・ユニット128、アンテナ126、制御ユニット130及び処理装置132を包含しており、これらは各々基地局B1の対応するセクションについて説明した機能を持っている。

【0028】本発明の1つの実施例では、暗号化されたメッセージをシステム100において途中で解読されることなく1つのユーザーから他のユーザーに渡すことができる。2移動局間、基地局及び移動局の間、及び、移動局と適宜の装備を持った陸線加入者局との間を含む、システム内の随意の2ポイント間でのポイント間通信を提供するためにこの実施例を使用することができる。

【0029】ポイント間メッセージ伝送を安全に行うために、システム100の各移動局Mxに、公然と知られ

る暗号化キーEmxと移動局Mxにおいてのみ知られる解読キーDmxとが割り当てられる。通信を希望している任意の2移動局M1及びM2について、Dm1Em2はEm2Dm1と等しくなければならない。しかし、M1及びM2の各々により使用される暗号化アルゴリズムは異なってもよい。MS1のユーザーがMS2のユーザーに機密保護通信メッセージcを送ることを希望しているとき、通信メッセージcはMS1においてEm1及びAm1で暗号化されて暗号化メッセージEm1(c)が作られる。MS1はこのEm1(c)をシステムの基地局B1に送る。基地局B1はEm2及びAm2を用いてEm1(c)を暗号化してメッセージEm2(Em1(c))を作り、これをMS1に送る。次にMS1はDm1及びAm1を用いてEm2(Em1(c))を解読する。Dm1Em2=Em2Dm1であるので、Dm1を用いてEm2(Em1(c))を解読するとEm2(c)が得られる。MS1はこのEm2(c)をB1に送る。B1はこのEm2(c)を、MS2が位置している地域を管理する基地局B2に送る。次にEm2(c)はMS2に送られて、MS2によってDm2及びAm2で解読されて、MS1によりMS2に送られる解読済み通信メッセージcが作られる。

【0030】ここで図2を参照すると、本発明の実施例の通信システム内でポイント間暗号化通信を行うために実行されるプロセスステップを示す流れ図が示されている。実例として、図1の移動局M1と移動局M2との間の暗号化メッセージ転送の場合を用いてこのプロセスを説明するが、M1はラビンのアルゴリズム(Rabin algorithm)を使用し、M2はライベスト、シャミル及びエイドルマン(RSA)のアルゴリズム(Rivest, Shamir and Adleman (RSA) algorithm)を使用する。ラビンのアルゴリズムについての予備的説明が、1995年にCRCにより刊行されたスティンソン(Stinson)の書籍“暗号法の理論と実際”(“Cryptography, Theory and Practice”)の143-148頁に記載されている。RSAアルゴリズムについての詳しい解説が1996年にジョン・ワイリー・アンド・サンズ(John Wiley and Sons)から刊行されたリンチ等(Lynch et al.)の書籍“デジタルマネー”(“Digital Money”)の76-86頁に記載されている。

【0031】移動局M1のためのキー関数Em1及びDm1をラビンの基準に従って選択することができる。ラビンのアルゴリズムでは、この例では、選択された所定の数Nを用いて2つの素数p及びqが選択され、ここで $p \times q = N$ であり、 $p = 4k_1 + 3$ であり、 $q = 4k_2 + 3$ であり、この $k_1$ 及び $k_2$ は定数である。Nは公然と知られてもよいが、p及びqは秘密に保たなければならない。Em1は $Em1(c) = (c)^2 \bmod N$ と定義され、Dm1は $DM1(c) = c^{1/2} \bmod N$ と定義され、このcは送信されるべきメッセージであ

る。DM1(c)を $c^{1/2}$ について解くために、解 $x_1 = \pm c^{(p+1)/4}$ 、及び $x_2 = \pm c^{(q+1)/4}$ を用いて方程式 $x^2 = c \pmod{p}$ と $x^2 = c \pmod{q}$ とを解く。2つの値a及びbが $ap + bq = 1$ となることが分かったならば、方程式 $c^{1/2} = bqx_1 + apx_2 \pmod{N}$ によって $c^{1/2}$ を発見することができる。

【0032】移動局M2についてのキー関数Em2、Dm2をライベスト、シャミル及びエイドルマン(RSA)の基準に従って選択することができる。RSAでは2つの(大きな)素数p及びqが始めに選択され、ここで $p \times q = N$ である。この実施例では、M2のためのNはM1のために使われるNに等しい。それ故に $Dm1Em2 = Dm2Em1$ という条件を満たすのが簡単である。しかし、 $Dm1Em2 = Em2Dm1$ である限りは、Nの他の値を使ってもよい。その場合、2つの他の値a2及びb2が選択され、ここで $(a2)(b2) = 1 \pmod{(p-1)(q-1)}$ である。N及びa2は公開されてもよく、b2は秘密に保たなければならない。このとき、Em2及びDm2は $Em2(c) = (c)^{a2} \pmod{N}$ 、及び $Dm2 = (c)^{b2} \pmod{N}$ と定義される。

【0033】プロセスはステップ200から始まり、ここで暗号化プロセスがM1で開始される。ステップ202において、Em1及びAm1を用いて論理ユニット112により通信メッセージcが暗号化されて暗号化メッセージEm1(c) =  $(c)^2 \pmod{N}$ が作られる。プロセスはステップ204に移行し、ここでEm1(c)はトランシーバー・ユニット104を通してM1からB1へ送信される。トランシーバー・ユニット136を通してEm1(c)を受け取った後、B1の処理装置140はステップ206でEm2及びAm2を用いてEm1(c)を暗号化して暗号化メッセージEm2(Em1(c)) =  $((c)^2)^{a2} \pmod{N}$ を作る。プロセスは次にステップ208に移り、ここでEm2(Em1(c))がB1からM1に送られる。次にステップ210において、B1からEm2(Em1(c))を受け取った後、M1の論理ユニット112は前記の様にAm2(ラビンのアルゴリズム)を用いてEm2(Em1(c))を解読する。 $(Em2(Em1(c)))^{1/2} = (((c)^2)^{a2})^{1/2}$ である。作られたDm1(Em2(Em1(c)))は $(c)^{a2} \pmod{N}$ 、即ち暗号化メッセージEm2(c)に等しい。

【0034】次に、ステップ212において、M1のトランシーバー・ユニット104は暗号化メッセージEm2(c)をB1に送る。次に、ステップ214において、B1の制御ユニット138は陸線通信網142を通してEm2(c)をB2の制御ユニット130に送る。このメッセージは暗号化されているので、これは安全な通信である。次にステップ216において、B2の制御ユニット130を通してEm2(c)を受け取った後、

トランシーバー・ユニット128はEm2(c)をM2に送る。ステップ218でEm2(c)はM2の処理装置132でDm2及びAm2を用いて解読されてDm2(Em2(c)) =  $(c)^{a2b2} \pmod{N}$ 、即ちDm2(Em2(c)) = cが作られる。このときM2は解読済み通信メッセージcを受け取ったことになる。

【0035】本発明の他の実施例では、システム100において1つのユーザーから他のユーザーにメッセージを転送するために非ポイント間法が使用される。この実施例では、送信側ユーザーと通信している基地局でそのメッセージが解読される。その後、そのメッセージは該メッセージの受取手と通信している基地局に送られて解読されて該メッセージの受取手に送られる。この実施例では、通信を行っている移動局或いは基地局の各々がそれ自身の暗号化キーと暗号化/解読アルゴリズムとを知っているだけで良い。通信を行っているエンティティは、通信を行っている他のいずれのエンティティの暗号化アルゴリズムを知らなくてもよいし、またそれを実行できなくてもよい。

【0036】一般に、この実施例では、各移動局Mxに暗号化キーEmxと解読キーDmxとが割り当てられる。Dmxは移動局xにおいてのみ知られる。システム100の各基地局Bxには暗号化キーEbxと解読キーDbxとが割り当てられる。Dbxは基地局Bxにおいてのみ知られる。互いに通信することを望んでいる移動局Mx及び基地局Byの任意の対について、DmxEbyはEbyDmxに等しくなければならない。

【0037】M1のユーザーが機密保護通信メッセージcをM2のユーザーに送ることを望んでいるとき、通信メッセージcはM1によりEm1及びAm1を用いて暗号化されてメッセージEm1(c)が作られる。M1はこのEm1(c)をシステムの基地局Bに送る。その後、基地局B1はEb1及びAb1を用いてEm1(c)を暗号化してメッセージEb1(Em1(c))を作り、これをM1に送る。次にM1はDm1及びA1を用いてEb1(Em1(c))を解読する。Dm1Eb1 = Db1Em1であるので、Dm1及びA2を用いてEb1(Em1(c))を解読するとEb1(c)が得られる。M1はこのEb1(c)をB1に送る。M1はこの時点でB1に正しいEb1(c)を送る唯一のユーザーであり得る。B1はDb1及びAb1を用いてEb1(c)を解読してcを作る。次にB1は、システムを通して、ユーザーM2が位置している地域を管理する基地局B2にcを送る。次にB2とM2との間で通信メッセージcはM1とB1との間での転送について述べたのと全く同様に暗号化され得るが、この場合、B2、Eb2、Db2及びAb2がM1、Em1、Dm1及びAm1に代わり、M2、Em2、Dm2及びAm2がB1、Eb1、Db1及びAb1に代わる。

【0038】図3を参照すると、本発明の実施例の通信



システム内で非ポイント間暗号化通信を提供するために  
行われるプロセスステップを示す流れ図が示されてい  
る。図3の流れ図を使って、図1の移動局M1と移動局  
M2との間での暗号化メッセージ転送の場合を説明する  
ことができる。この例では、M1及びM2はラビンのアル  
ゴリズムを使用し、B1及びB2はRSAアルゴリズム  
を使用する。図3で使用するプロセスでは、M1及  
びM2は基地局で使用するRSAアルゴリズムを使用  
しなくてもよい。

【0039】移動局Myのキー関数Emy、Dmyはラ  
ビンの基準に従って選択され得る。この例についてのラ  
ビンのアルゴリズムでは、選択された数Nを用いて2つ  
の素数p及びqが選択され、ここで $p \times q = N$ であり、  
 $p = 4k_1 + 3$ であり、 $q = 4k_2 + 3$ であり、 $k_1$ 及  
び $k_2$ は定数である。Nは公然と知られてもよく、p及  
びqは秘密に保たなければならない。Emyは $E_{m1}(c) = (c)^2 \bmod N$ と定義され、DMyは $D_{m1}(c) = c^{1/2} \bmod N$ と定義される。DMy  
(c)をcについて解くために、解 $x_1 = \pm c^{(p+1)/4}$ 、及び、 $x_2 = \pm c^{(q+1)/4}$ を用いて方程式  
 $x^2 = c \bmod p$ 、及び、 $x^2 = c \bmod q$ を  
解く。2つの値a及びbが $ap + bq = 1$ であることが  
分かったならば、方程式 $c^{1/2} = bqx_1 + apx_2$   
 $\bmod N$ によりcを見いだすことができる。

【0040】基地局xについてのキー関数Ebx及びD  
bxをライベスト、シャミル及びエイドルマン(RS  
A)の基準に従って選択することができる。RSAで  
は、始めに2つの(大きな)素数p及びqが選択され、  
ここで $p \times q = N$ である。次に他の2つの値ax及びb  
xが選択され、ここで $(ax)(bx) = 1 \bmod (p-1)(q-1)$ である。Ebx及びDbxは、  
 $E_{bx}(c) = (c)^{ax} \bmod N$ 、 $D_{bx}(c) = (c)^{bx} \bmod N$ と定義される。この実施例では、B1につ  
いてのNはM1に使用されるNに等しく、B2につ  
いてのNはM2に使用されるNに等しい。それ故に、 $D_{m1}E_{b1} = E_{b1}D_{m1}$ という条件を満たすのが容易にな  
る。しかし、 $D_{m1}E_{b1} = E_{b1}D_{m1}$ であり、且つ  
 $D_{m2}E_{b2} = E_{b2}D_{m2}$ である限りは、Nの他の値  
を使用してもよい。

【0041】プロセスはステップ300から始まり、こ  
こで暗号化プロセスが開始される。次にステップ302  
で、通信メッセージcはM1の論理ユニット112でE  
m1及びAm1を用いて暗号化され、暗号化メッセージ  
 $E_{m1}(c) = (c)^2 \bmod N$ が作られる。次にス  
テップ304に移行し、ここで $E_{m1}(c)$ はトランシー  
バー・ユニット104を通してM1からB1に送られ  
る。ステップ306で、トランシーバー・ユニット13  
6を通して $E_{m1}(c)$ を受け取った後、B1はE b 1  
及びA b 1を用いて $E_{m1}(c)$ を暗号化して、暗号化  
メッセージ $E_{b1}(E_{m1}(c)) = ((c)^2)^{a1}$

$\bmod N$ を作る。プロセスは次にステップ308に移  
行し、ここで $E_{m2}(E_{m1}(c))$ はトランシーバー  
・ユニット136を通してM1からB1に送られる。次  
に、ステップ310において、トランシーバー・ユニッ  
ト104を通してB1から $E_{m2}(E_{m1}(c))$ を受  
け取った後、前述したようにM1の論理ユニット112  
は $D_{m1}$ 及びラビンのアルゴリズムを用いて $E_{b2}(E_{m1}(c))$ を解読する。 $E_{b2}(E_{m1}(c))$   
 $^{1/2} = (((c)^2)^{a2})^{1/2}$ 。作られたメッセージ $D_{m1}(E_{b2}(E_{m1}(c)))$ は $(c)^{a2} \bmod N$ 、即ち暗号化メッセージ $E_{b2}(c)$ に等しい。

【0042】次に、ステップ312において、M1はト  
ランシーバー・ユニット104を通して暗号化メッセ  
ージ $E_{b1}(c)$ をB1に送り、ステップ314において  
B1の処理装置140は $D_{b1}$ を用いて $E_{b1}(c)$ を  
解読して $D_{b1}(E_{b1}(c)) = ((c)^{a1})^{b1} \bmod N = c$ を作る。処理装置140で通信メッセージc  
が解読された後、プロセスはステップ316に移行し、  
ここで通信メッセージcは基地局B1の制御ユニット1  
38から陸線通信網142を通して基地局B2の制御ユ  
ニット130に送られる。B2とM2との間の通信メ  
ッセージcの伝送は、M1及びB1の間での転送につ  
いて述べたのと全く同様に行われ得る。それはステ  
ップ318-330で説明されており、それらはステ  
ップ302-314と同一であり、B2、 $E_{b2}$ 、 $D_{b2}$ 及び  
 $A_{b2}$ がM1、 $E_{m1}$ 、 $D_{m1}$ 及び $A_{m1}$ に代わり、  
M2、 $E_{m2}$ 、 $D_{m2}$ 及び $A_{m2}$ がB1、 $E_{b1}$ 、 $D_{b1}$   
及び $A_{b1}$ に代わる。

【0043】本発明の教示内容は前記の通信規格での使  
用のみに限定されると解されてはならず、類似の如何な  
るシステムをも包含すると解されるべきである。更に、  
上で明示的に開示した暗号化アルゴリズム以外の暗号化  
アルゴリズムを使用して本発明を実施してもよい。

【0044】本発明は、その好ましい実施例に関して具  
体的に図示され解説されており、本発明の範囲から逸脱  
することなく形及び細部に変更を加え得ることが当業者  
に理解されるであろう。

【図面の簡単な説明】

【図1】本発明の実施例に従って構成された通信シス  
テムのブロック図である。

【図2】本発明の実施例の通信システム内でポイント間  
暗号化通信メッセージを提供するために行われるプロセ  
スステップを示す流れ図である。

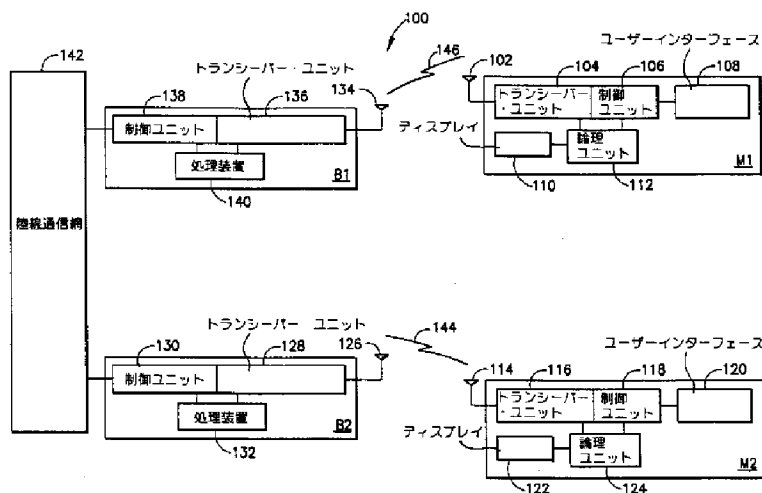
【図3】本発明の実施例の通信システム内で非ポイント  
間暗号化通信メッセージを提供するために行われるプロ  
セスステップを示す流れ図である。

【符号の説明】

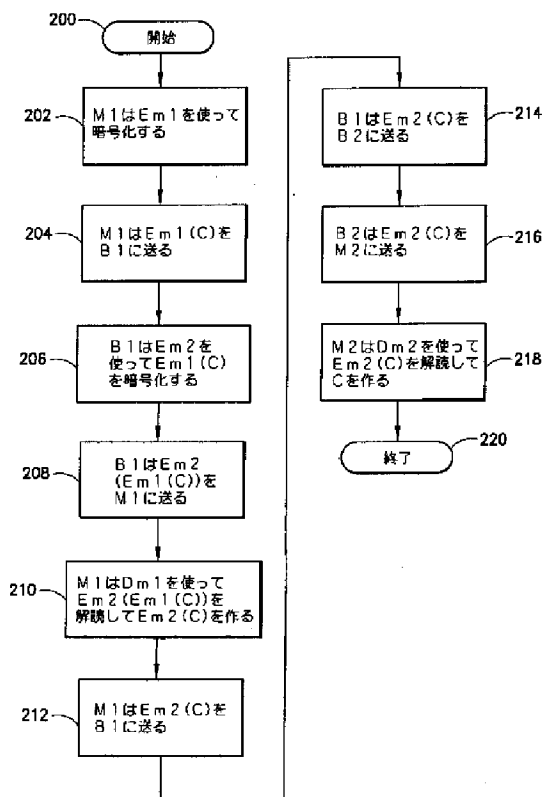
B1、B2…基地局

M1、M2…移動局

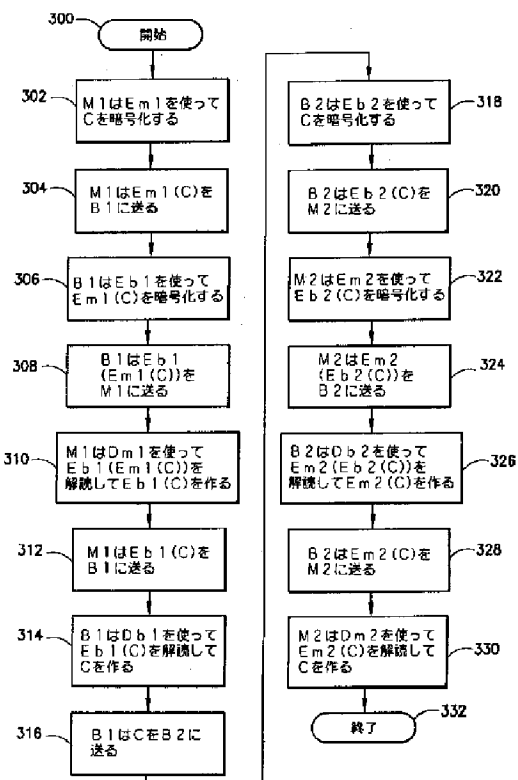
【図1】



【図2】



【図3】





US005909491A

**United States Patent** [19][11] **Patent Number:** **5,909,491****Luo**[45] **Date of Patent:** **Jun. 1, 1999****[54] METHOD FOR SENDING A SECURE MESSAGE IN A TELECOMMUNICATIONS SYSTEM**[75] Inventor: **Tie Luo**, Arlington, Tex.[73] Assignee: **Nokia Mobile Phones Limited**, Espoo, Finland[21] Appl. No.: **08/744,682**[22] Filed: **Nov. 6, 1996**[51] Int. Cl.<sup>6</sup> ..... **H04L 9/08**[52] U.S. Cl. .... **380/21; 380/30; 380/49; 455/410**

[58] Field of Search ..... 455/26, 410; 380/30, 380/49, 21

**[56] References Cited****U.S. PATENT DOCUMENTS**

4,411,017 10/1983 Talbot ..... 455/411

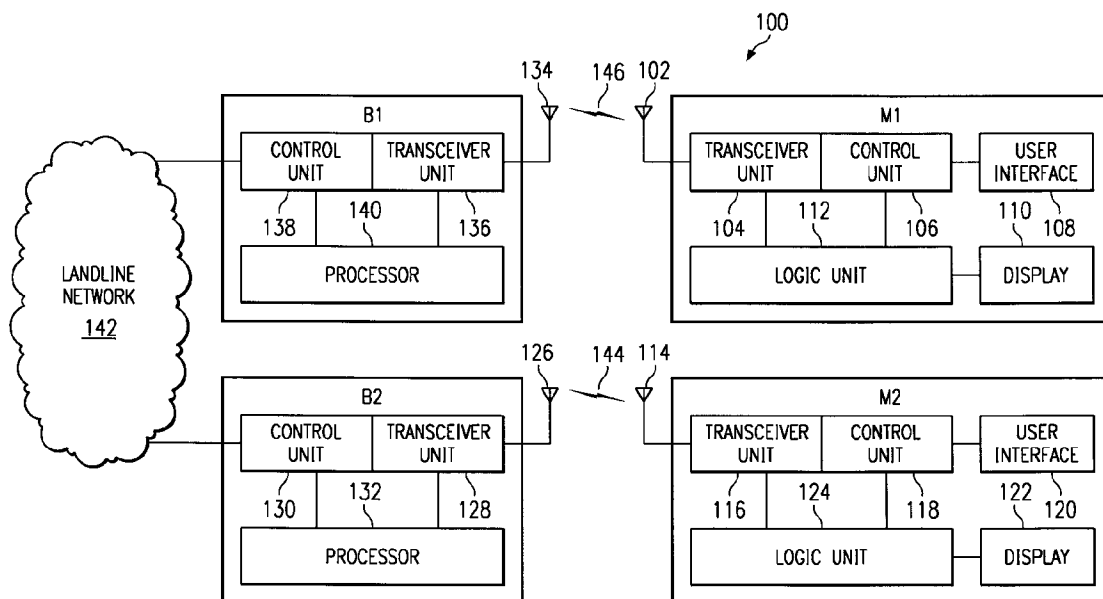
**OTHER PUBLICATIONS**

Bruce Schneier, Applied Cryptography, Book, pp. 516–517, Oct. 18, 1995.

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, Chapter 8, Oct. 1996.

*Primary Examiner*—Gail O. Hayes*Assistant Examiner*—Ho S. Song*Attorney, Agent, or Firm*—Brian T. Rivers**[57] ABSTRACT**

A method for sending a secure message in a telecommunications system using public encryption keys. A sending transceiver encrypts the message  $c$  using the sender's own public encryption key  $Ex$  to generate  $Ex(c)$ , and, transmits the encrypted message  $Ex(c)$  to a receiving transceiver. The receiving transceiver then encrypts the encrypted message  $Ex(c)$  using the encryption key  $Ey$  of the intended receiver of the message to generate the message  $Ey(Ex(c))$ , and, transmits the message  $Ey(Ex(c))$  back to the sending transceiver. The sending transceiver then decrypts the message  $Ey(Ex(c))$  using sender's private decryption key to generate  $Dx(Ey(Ex(c)))=Ey(c)$ , and, transmits the message  $Ey(c)$  back to the receiving transceiver. The receiving transceiver then either decrypts the message using its own decryption key  $Dy$ , if it is the intended receiver of the message, to generate  $Dy(Ey(c))=c$ , or, forwards the message on to the intended receiver of the message, where the intended receiver decrypts the message using its own decryption key  $Dy$ .

**10 Claims, 2 Drawing Sheets**

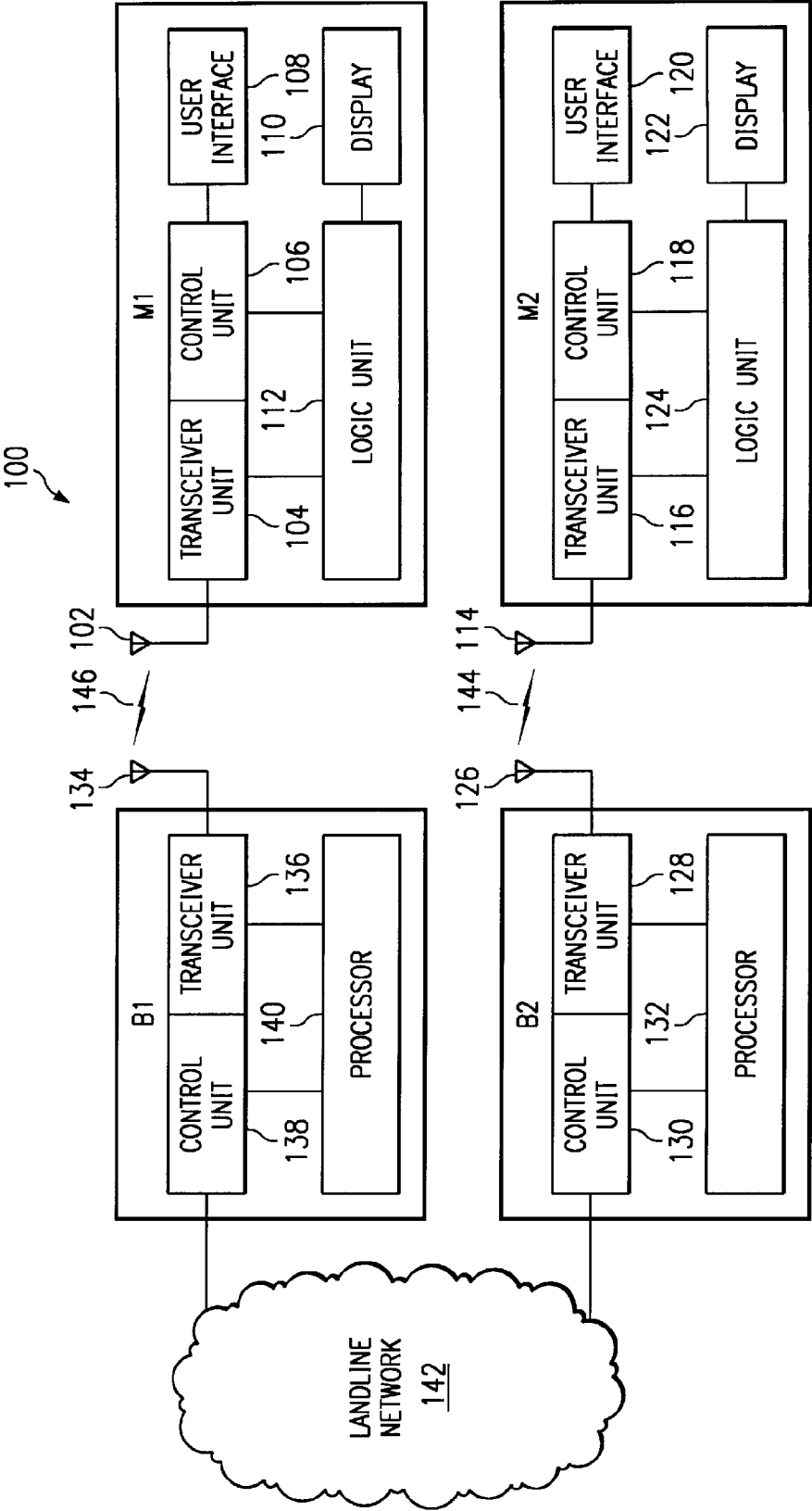


FIG. 1

FIG. 2

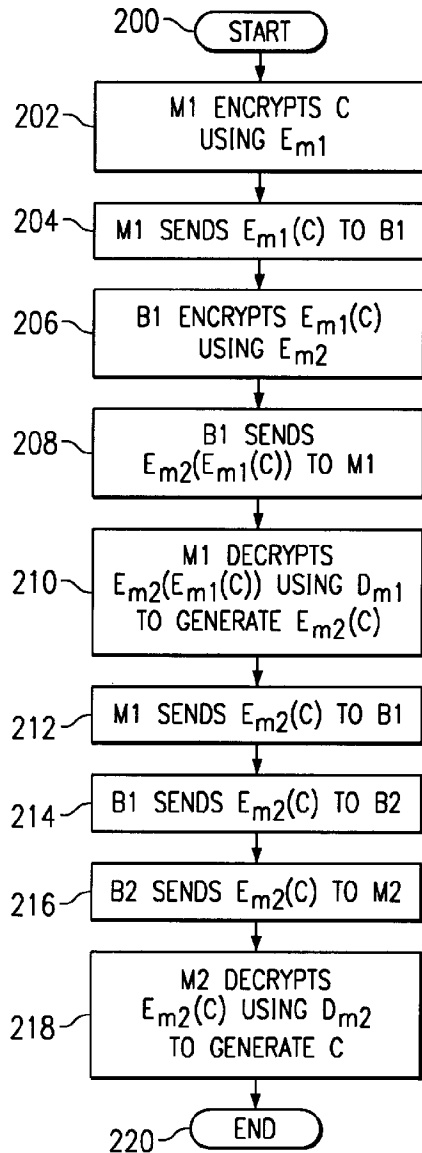
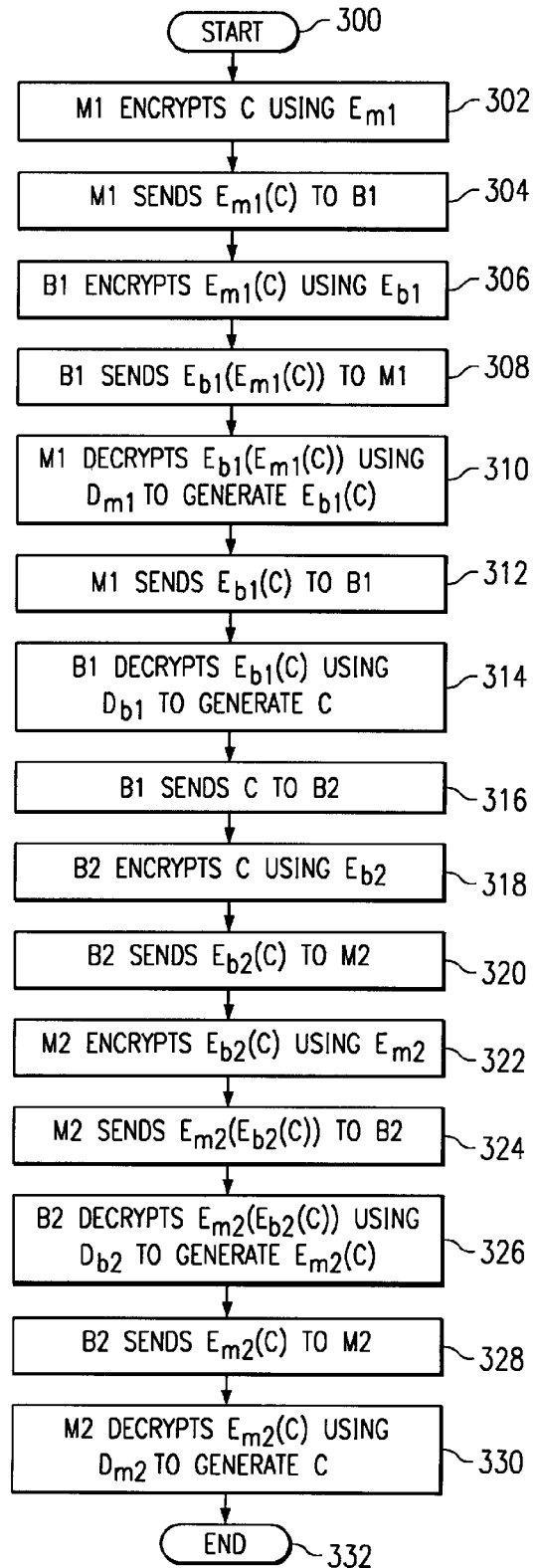


FIG. 3



# METHOD FOR SENDING A SECURE MESSAGE IN A TELECOMMUNICATIONS SYSTEM

## FIELD OF THE INVENTION

This invention relates to encryption techniques for telecommunications systems and, more particularly, to an apparatus and method for sending a secure message in a telecommunications system using public encryption keys.

## BACKGROUND OF THE INVENTION

Advances in telecommunications systems technology have resulted in a variety of telecommunications systems and services being available for use. These systems include cellular telephone networks, personal communications systems, various paging systems, and various wireline and wireless data networks. Cellular telephone networks currently in use in the United States include the AMPS analog system, the digital IS-136 time division multiplexed (TDMA) system, and the digital IS-95 digital code division multiplexed (CDMA) system. In Europe the Global Services for Mobile (GSM) digital system is most widely used. These cellular systems operate in the 800–900 Mhz range. Personal communications systems (PCS) are also currently being deployed in the United States. Many PCS systems are being developed for the 1800–1900 MHz range, with each based on one of the major cellular standards.

In each of the above mentioned telecommunications systems, it may often be desirable for the operators of the system to provide secure communications to users of the system. This may include sending a secure message between two mobile stations operating in the system. In many cases the message may be a text message of finite length, such as a text message.

In analog systems, such as AMPS, it is very difficult to provide security for communications. The analog nature of the signals carrying the communication between two users does not permit easy or efficient encryption. In fact, in standard AMPS, no encryption is used and communications sent between a mobile station and base station may be monitored and intercepted. Anyone having a receiver capable of tuning to the frequencies used for the communication channels may intercept a message at anytime, without being detected. The possibility of interception has been one negative factor connected with analog systems such as AMPS. Because of this potential for interception, AMPS type systems have not been favored for certain business or governmental uses, where sending a secure message is a requirement.

The newer digital systems such as GSM, IS-136, and IS-95 have been developed so as to include encryption services for communications privacy. The digital nature of the speech or data signals carrying the communications between two users in these digital systems allows the signals to be processed through an encryption device to produce a communications signal that appears to be random or pseudorandom in nature, until it is decrypted at an authorized receiver. When it is desired to send a secure message in such a system, the encryption feature of the system can be used to encrypt the message. As an example, the short message service (SMS) feature specified in these standards could be used to send a text message that is encrypted according to the system encryption algorithm.

In the GSM, IS-136, and IS-95 systems, the encryption is performed on message transmissions between each user and the system by using a secret key value, "private key", where

the key is known only to the system and the user communicating with the system. The system standards under consideration for PCS networks may also include encryption services that are based on the encryption techniques specified in the digital standard from which a particular PCS standard is derived, i.e., GSM, IS-136, or IS-95.

In GSM the system operator controls the security process by issuing a subscriber identity module (SIM) to each system user. The SIM is a plug-in chip or card that must be inserted into a mobile station that a user intends to make or receive calls through. The SIM contains a 128 bit number called the Ki that is unique for each user. The Ki is used for both authentication and deriving an encryption key. In GSM a challenge and response procedure is used to authenticate each user and generate encryption bits from Ki for the user. The challenge and response procedure may be executed at the discretion of the home system.

When a GSM mobile is operating in its home system, after the user has identified himself by sending in his international mobile system identity/temporary mobile system identities (IMSI/TMSI), a 128-bit random number (RAND) is generated in the system and combined with the mobile user's Ki to generate a 32-bit response (SRES). The system then transmits RAND to the mobile which, in turn, computes its own SRES value from the mobile user's Ki, and transmits this RAND back to the system. If the two SRES values match, the mobile is determined to be authentic. Encryption bits for communications between the mobile and systems are generated in both the mobile and network by algorithms using RAND and Ki to produce an encryption key "Kc". Kc is then used at both ends to provide secure communications. When a GSM mobile is roaming, the RAND, SRES and Kc values are transferred to a visited system upon registration of the user in the visited system or, upon a special request from a visited system. The Ki value is never available other than in the home system and the user's SIM.

The IS-136 and IS-95 authentication and encryption procedures are identical to each other and, similar to the GSM authentication and encryption procedures. In IS-136 and IS-95 systems a challenge response method is also utilized. The IS-136 and IS-95 method utilizes a security key called the "A-key". The 64-bit A-key for each mobile is determined by the system operators. The A-key for each mobile is stored in the home system of the mobile's owner and in the mobile itself. The A-key may be initially communicated to the mobile owner in a secure manner, such as the United States mail. The owner can then enter the A-key into the mobile via the keypad. Alternately, the A-key may be programmed into the mobile station at the factory or place of service. The A-key is used to generate shared secret data (SSD) in both of the mobile and the home system from a predetermined algorithm. SSD for each mobile may be periodically derived and updated from the A-key of that particular mobile by use of an over the air protocol that can only be initiated by the home system operator.

In IS-136 and IS-95 authentication and encryption, a 32-bit global challenge is generated and broadcast at predetermined intervals within systems in the service area of the mobile. When a mobile attempts system registration/call setup access in the home system, the current global challenge response is used to compute, in the mobile, an 18-bit authentication response from the mobile's SSD. An access request message, including the authentication response and a call count value for the mobile, is then sent to the home system from the mobile. Upon receiving the access request the home system will compute its own response value using

the global challenge and the mobile's SSD. If the mobile is verified as authentic, by comparison of the authentication responses, the mobile's SSD and other relevant data, including the call count value, the mobile is registered.

When a mobile attempts system registration/call setup access in a visited system, the current global challenge response is used to compute, in the mobile, the 18-bit authentication response from the mobile's SSD. An access request message is then sent to the visited system from the mobile. For initial registration accesses in a visited system, the access request message includes the authentication response computed in the mobile. The authentication response and global challenge are then sent to the home system of the mobile, where the home system will compute its own response value using the global challenge and the mobile's SSD. If the mobile is verified as authentic, by comparing the authentication responses, the mobile's SSD and other relevant data, including the call count value, is then sent to the visited system and the mobile is registered. When a call involving the mobile is setup, a current authentication response value and call count are sent to the system from the mobile along with the call setup information. Upon receiving the call setup information, the visited system retrieves the stored SSD and call count values for the requesting mobile. The visited system then computes an authentication response value to verify that the received SSD value and the current global challenge produce the same response as that produced in the mobile. If the authentication responses and call counts match, the mobile is allowed call access. If communications security is desired, an encryption key is produced in both the mobile and system by using the global challenge and the mobile's SSD as input to generate encryption key bits.

Further background for such techniques as those used in GSM and, the IS-136 and IS-95 systems may be found in the article "Techniques for Privacy and Authentication in Personal Communications Systems" by Dan Brown in IEEE Personal Communications, dated August 1995, at pages 6-10.

While the above described private key procedures used in the GSM, IS-136 and IS-95 systems provide communications security, none of these procedures is entirely immune to interception and eavesdropping. All of the procedures require that a user's A-key or Ki value be known both in the mobile station and home system. They also require that the user's SSD or Kc value be known at both ends of the communications link, i.e., in the system and in the mobile. Each of these values could potentially be corrupted and become known to a potential interceptor. An individual knowing the Ki or A-key of a user, or an individual who intercepts the Kc or SSD of the user in intersystem communications, could potentially intercept and eavesdrop on communications that were intended to be secure and private. Additionally, since each user's keys are available at a base station with which they are communicating, encrypted communications involving two mobile stations connected through a base station of a system could be breached at the base station.

Public key encryption methods are methods in which a user is assigned an encryption key that is public, i.e., may be known and revealed publicly, but is also assigned a private decryption key that is known only to the user. Only an intended receiving user's decryption key can decrypt an encrypted message meant for the intended receiving user, i.e., decrypt a message encrypted using the intended receiving user's encryption key. In a public key encryption telecommunication system, the user would be allowed to keep

the decryption key to himself, away from base stations or the system. Since the key necessary for decrypting a message is known only to the receiving user, public key encryption methods could provide more secure communications than are obtainable with the current encryption techniques being, used in, for example, GSM, IS-136, or IS-95.

In a cellular system using conventional public key encryption, if a mobile station X were to send an encrypted message to mobile station Y, mobile station X is required to know both the public encryption key for mobile station Y and, the algorithm that must be used with the encryption key of mobile station Y. It would also be required that Mobile X be capable of performing the encryption of the message using mobile station Y's encryption key and algorithm. These requirements of conventional public key encryption may present some difficulties or not be quite optimal for use in cellular systems in certain situations.

One difficulty in using public key encryption techniques is that the calculations involved in encryption and decryption may require much more in the way of computational resources than is required by private key systems. In a mobile station such computational resources may be limited. The requirements on resources may be even greater if two mobile station users desire to exchange a message securely, with each user using a different encryption/decryption algorithm. This could be the case, for example, when a roaming mobile station enters a system in which the system operator has implemented his own unique algorithm that is different from the roaming mobile station's home system's algorithm. In this case, each particular mobile station would be required to be capable of performing encryption with the other user's algorithm and, decryption with that particular mobile station user's algorithm. Such a requirement could be difficult to meet, for example, if the algorithm used for encryption required more computational resources than were available in the mobile station performing the encryption. Also, the code and data for performing particular algorithms would have to be stored in each mobile station or transmitted to the mobile station prior to commencement of encryption, creating further demands on mobile station computational resources.

Another potential difficulty in using public key encryption techniques in a cellular system involves the requirement that the sending mobile station should know the encryption key of the receiving mobile station in order to assure that the message is only available to the sending or receiving mobile stations. In certain public key encryption techniques the encryption keys may each be very large, possibly a sequence of numbers, and it may be difficult to store encryption keys for all potential receiving mobile stations in a single mobile station. It may also be difficult to transmit the key of a receiving mobile station to a sending mobile station on an as needed basis, for example during call setup, if the key is very large.

#### SUMMARY OF THE INVENTION

The present invention provides a method for sending a secure message in a telecommunications systems using public key encryption. The method is implemented in such a way that a particular user's decryption key is known only at the transceiving device of the particular user. The method is also implemented so that the transceiving device of the particular user needs only be capable of using that particular user's encryption/decryption algorithm and encryption key. This is done by using a particular sequence to exchange messages between two transceiving devices. The method

avoids security problems associated with using private key methods and, also allows each mobile station to be able to perform only its own public key encryption/decryption algorithm. The method does not require that a transceiving device be able to perform encryption using the encryption key and algorithm of an intended receiver transceiving device as in conventional public key encryption. Computational resources in a transceiving device can therefore be optimized for one particular algorithm.

The method may be useful in providing highly secure, short message service (SMS) teleservices when a secure message is exchanged between two mobile stations or a mobile station and a cellular network, with each mobile station or the network using a different encryption/decryption algorithm. The method may also be useful in exchanging private keys between two communicating mobile stations or, a mobile station and a network, so that less computationally intensive private key algorithms may be used for longer communications, such as voice transmission. Additionally, the method may be used to transmit a secure authentication signature from one mobile station to another mobile station or network.

In an embodiment of the invention, a method for point to point encryption of a message exchanged between two users is implemented into a telecommunications system having at least one base station and a plurality of mobile stations. In the point to point embodiment, no decryption is performed in the base stations of the system. A user of mobile station M1 is assigned a publicly known (known to the system) encryption key Em1 and a decryption key Dm1 that is known only at mobile station M1 (the terms "encryption key Emx" and "decryption key Dmx" will be used herein to refer to both the algorithm and key values used in the algorithm, i.e., Emx is the encryption/decryption algorithm using the encryption key values and Dmx is the encryption/decryption algorithm using the decryption key values). Another system user of mobile station M2 is assigned a publicly known encryption key Em2 and a decryption key Dm2 that is known only at mobile station M2, where  $Dm1Em2=Em2Dm1$ .  $Dm1Em2=Em2Dm1$  sets the restriction that applying Dm1 first to a message and then applying Em2, is the same as applying Em2 first and then Dm1 to the message. Only M1 knows Dm1 and only M2 knows Dm2. Also, M1 needs only to know Em1 and M1's particular encryption/decryption algorithm (A1) and, M2 needs only know Em2 and M2's particular encryption algorithm (A2).

When a user having mobile station M1 desires to send a secure communication c to a user of mobile station M2, the communication c is encrypted at M1 using Em1 and A1 to generate a message Em1(c). M1 then sends Em1(c) to a base station B1 of the system. The base station B1 then encrypts Em1(c) using Em2 and A2 to generate the message Em2(Em1(c)) and sends it back to M1. Em2(Em1(c)) is next decrypted at M1 using Dm1 and A1. Since  $Dm1Em2=Em2Dm1$ , decrypting Em2(Em1(c)) using Dm1 results in Em2(c). M1 then sends Em2(c) to B1. B1 now sends Em2(c) to base station B2 that controls the area where mobile station M2 is located. Em2(c) is next sent to mobile station M2 and decrypted by mobile station M2 using Dm2 and A2 to generate the communication c sent by mobile station M1 to mobile station M2.

In another embodiment of the invention, a method of non-point to point encryption of communications between two mobile stations may be implemented into a telecommunications system. A system user of mobile station M1 is assigned a publicly known (known to the system) encryption key Em1 and a decryption key Dm1 that is known only at

mobile station M1. M1 uses an encryption/decryption algorithm A1. Another system user of mobile station M2 is assigned a publicly known encryption key Em2 and a decryption key Dm2 that is known only at mobile station M2. M2 uses an encryption/decryption algorithm A2. Also, each base station Bx of the system is assigned a publicly known encryption key Ebx and a decryption key Dbx that is known only to base station Bx. Each base station also performs encryption/decryption according to an algorithm Abx. The keys are chosen so that for any pair of a base station Bx and mobile station Mx which may communicate with each other,  $DmxEbx=EbxDmx$ .

In this embodiment, when user having mobile station M1 desires to send a secure communication c to a user of mobile station M2, the communication c is encrypted at M1 using Em1 and A1 to generate a message Em1(c). M1 then sends Em1(c) to a base station B1 of the system. The base station B1 then encrypts Em1(c) using Eb1 and Ab1 to generate the message Eb1(Em1(c)) and sends it back to M1. Eb1(Em1(c)) is next decrypted at M1 using Dm1 and A1. Since  $Dm1Eb2=Eb2Dm1$ , decrypting Eb1(Em1(c)) using Dm1 results in Eb1(c). M1 then sends Eb1(c) to B1. B1 then decrypts Eb1(c) using Db1 and Ab1 to generate c and, sends c to a base station B2 that controls the area where mobile station M2 is located. The communication c between B2 and M2 may then be encrypted in an identical manner to that described for the transfer between M1 and B1, with B2, Eb2, Db2 and Ab2, in place of M1, Em1, Dm1 and A1, and, M2, Em2, Dm2 and A2, in place of B1, Eb1, Db1 and Ab1.

#### BRIEF DESCRIPTION OF THE DRAWINGS

A more complete understanding of the method of the present invention may be had by reference to the following detailed description when read in conjunction with the accompanying drawings wherein:

FIG. 1 illustrates a block diagram of a telecommunications system constructed according to an embodiment of the invention;

FIG. 2 is a flow diagram showing process steps performed to provide point to point encrypted communications within a telecommunications system according to an embodiment of the invention; and

FIG. 3 is a flow diagram showing process steps performed to provide non point to point encrypted communications within a telecommunications system according to an embodiment of the invention.

#### DETAILED DESCRIPTION OF THE INVENTION

FIG. 1 illustrates a block diagram of a telecommunications system 100 constructed according to an embodiment of the invention. System 100 comprises base stations B1 and B2, land line network 142, and mobile stations M1 and M2. Although shown to include two base stations and two mobile stations, system 100 may comprise more or less base stations or mobile stations than are shown in FIG. 1. The mobile stations M1 and M2 may be mobile telephones that provide speech communications between a user of M1 or M2, and another mobile telephone or, between the user and a land line telephone connected to landline network 142. Mobile stations M1 and M2 may also be any other type of mobile communications device capable of operating according to the system standard for system 100, such as a personal communications device or a laptop computer operating through a wireless modem. Landline network 142 may be a public switched telephone network (PSTN) or a private land-



line network for system 100 that includes mobile switching centers for controlling call routing, registration and hand-off of a mobile from one base station to another in system 100. In system 100, mobile stations M1 and M2 may move about the coverage area of system 100 while communicating with the base stations of system 100 through RF links. In FIG. 1, mobile stations M1 and M2 are shown to be communicating with base stations B1 and B2, respectively, over RF links 144 and 146, respectively. System 100 may operate according to any telecommunications system standard that provides a digital interface over the RF links between mobile stations M1 and M2, and base stations B1 and B2. The design and operation of digital telecommunications systems is known and will not be described in detail here. System 100 may be implemented in any number of ways. For example, the digital RF interface in system 100 may operate according to a standard similar to the Telecommunications Industry Association/Electronic Industry Association (TIE/EIA) IS-136, IS-95, and PCS 1900 standards or the European GSM standard.

Mobile station M1 includes a transceiver unit 104 coupled to an antenna 102 for receiving radio signals from, and for transmitting radio signals to, base stations of system 100. Mobile station M1 includes a user interface 108, which could be a computer keyboard or a mobile telephone handset with a keypad, microphone and earpiece. Control unit 106 in mobile station M1 controls RF channel selection and other system functions in the conventional manner and, a logic unit 112 controls the general operation of the mobile station. Logic unit 112 may also be utilized to implement and perform encryption and decryption functions used for communications security. Display 110 provides a general visual interface to the user of mobile station M1 and is under control of logic unit 112. Mobile station M2 includes transceiver unit 116, user interface 120, control unit 118, logic unit 124, and display 122, each having the function as described for the corresponding section of mobile station M1.

Base station B1 includes a transceiver unit 136 coupled to antenna 134 for receiving radio signals from and, transmitting radio signals to mobile stations. B1 also includes control unit 138 and processor 140. Control unit 138 controls RF channel selection and assignment by generating the appropriate control messages to mobile stations, and also controls other necessary system functions such as interfacing with landline network 142. Processor 140 may be utilized to implement and perform encryption and decryption functions used for communications security. Base station B2 includes transceiver unit 128, antenna 126, control unit 130 and processor 132, each having the function as described for the corresponding section of base station B1.

In an embodiment of the invention an encrypted message may be passed from one user to another user in system 100, without the message being decrypted along the path from user to user. The message may only be decrypted by the intended receiver. The embodiment may be used to provide point to point communications between any two points in the system, including between two mobile stations, between a base station and a mobile station, and, between a mobile station and an appropriately equipped landline subscriber station.

For secure point to point message transmission, generally, each mobile station Mx of system 100 is assigned a publicly known encryption key Emx and a decryption key Dmx that is known only at mobile station Mx. For any two mobile stations M1 and M2 desiring to communicate, Dm1Em2 must equal Em2Dm1. However, the encryption algorithms

used by each of M1 and M2 may be different. When the user of MS1 desires to send a secure communication c to a user of MS2, the communication c is encrypted at MS1 using Em1 and Am1 to generate an encrypted message Em1(c). MS1 then sends Em1(c) to base station B1 of the system. The base station B1 then encrypts Em1(c) using Em2 and Am2 to generate the message Em2(Em1(c)) and sends it back to MS1. MS1 next decrypts Em2(Em1(c)) using Dm1 and Am1. Since Dm1Em2=Em2Dm1, decrypting Em2(Em1(c)) using Dm1 results in Em2(c). MS1 then sends Em2(c) to B1. B1 now sends Em2(c) to base station B2 that controls the area where MS2 is located. Em2(c) is next sent to MS2 and decrypted by MS2 using Dm2 and Am2 to generate the decrypted communication c sent by MS1 to MS2.

Referring now to FIG. 2, therein is illustrated a flow diagram showing process steps performed to provide point to point encrypted communications within a telecommunications system according to an embodiment of the invention. As an illustrative example, the case of a encrypted message transfer between mobile station M1 and mobile station M2 of FIG. 1 will be used to describe the process, with M1 using the the Rabin algorithm and, M2 using the Rivest, Shamir and Adleman (RSA) algorithm. A background description of the Rabin algorithm is given in the book "Cryptography, Theory and Practice" by Stinson, published by CRC, 1995, at pages 143-148. A detailed description of the RSA algorithm is given in the book "Digital Money" by Lynch et al., published by John Wiley and Sons, 1996, at pages 76-86.

The key functions Em1 and Dm1 for mobile station M1 may be chosen according to the Rabin criteria. In the Rabin algorithm, for this example, two prime numbers p and q are chosen using a selected predefined number N, where  $p \times q = N$ , and  $p = 4k_1 + 3$ , and,  $q = 4k_2 + 3$ , and where  $k_1$  and  $k_2$  are constants. N may be publicly known, while p and q must be kept private. Em1 is defined as  $Em1(c) = (c)^2 \text{ mod } N$  and, Dm1 is defined as  $Dm1(c) = c^{1/2} \text{ mod } N$ , where c is the message to be transmitted. To solve Dm1(c) for  $c^{1/2}$ , the equations  $x^2 = c \text{ mod } p$ , and,  $x^2 = c \text{ mod } q$ , are solved using the solutions,  $x_1 = \pm c^{(p+1)/4}$ , and,  $x_2 = \pm c^{(q+1)/4}$ . If two values a and b are found such that  $ap + bq = 1$ , then  $c^{1/2}$  can be found by the equation  $c^{1/2} = bq x_1 + ap x_2 \text{ mod } N$ .

The key functions Em2, Dm2, for mobile station M2 may be chosen according to the Rivest, Shamir and Adleman (RSA) criteria. In RSA two (large) prime numbers p and q are first selected, where  $p \times q = N$ . In this embodiment, N for M2 equals the N used for M1. This simplifies meeting the condition that  $Dm1Em2 = Dm2Em1$ . However other values of N could be used as long as  $Dm1Em2 = Em2Dm1$ . Two other values, a2 and b2, are then chosen, where  $(a2)(b2) = 1 \text{ mod } (p-1)(q-1)$ . N and a2 may be public, and b2 must be kept private. Em2 and Dm2 are then defined as  $Em2(c) = (c)^{a2} \text{ mod } N$ , and,  $Dm2 = (c)^{b2} \text{ mod } N$ .

The process starts at step 200 where the encryption process is initiated in M1. At step 202, communication c is encrypted by logic unit 112 using Em1 and Am1, to generate the encrypted message  $Em1(c) = (C)^2 \text{ mod } N$ . The process then moves to step 204 where Em1(c) is transmitted through transceiver unit 104 from M1 to B1. After receiving Em1(c) through transceiver unit 136, processor 140 of B1 encrypts Em1(c) at step 206, using Em2 and Am2, to generate the encrypted message  $Em2(Em1(c)) = ((c)^2)^{a2} \text{ mod } N$ . The process then moves to step 208 where  $Em2(Em1(c))$  is sent back to M1 from B1. Next at step 210, after receiving  $Em2(Em1(c))$  from B1, logic unit 112 of M1 decrypts  $Em2(Em1(c))$  using Am2 (the Rabin algorithm) as described before.  $(Em2(Em1(c)))^{1/2} = (((c)^2)^{a2})^{1/2}$ . The generated message  $Dm1(Em2(Em1(c)))$  then equals  $(c)^{a2} \text{ mod } N$ , or the encrypted message  $Em2(c)$ .

Next, at step 212, transceiver unit 104 of M1 sends the encrypted message Em2(c) to B1. Next, at step 214, control unit 138 of B1 then sends Em2(c) through landline network 142 to control unit 130 of B2. Since the message is encrypted, this is a secure communication. Next at step 216, after receiving Em2(c) through control unit 130 of B2, transceiver unit 128 sends Em2(c) to M2. At step 218 Em2(c) is decrypted in logic unit 124 of M2 using Dm2 and Am2 to generate  $Dm2(Em2(c))=((c)^{a^2})^{b^2} \bmod N$ , or,  $Dm2(Em2(c))=c$ . M2 now has received the decrypted communication c.

In another embodiment of the invention, a non-point to point method is used to transfer a message from one user to another user in system 100. In this embodiment the message is decrypted at the base station in communication with the sending user. The message is then sent to the base station in communication with the receiver of the message and encrypted for transmission to the receiver of the message. In this embodiment, each of the communicating mobile stations or base stations need only know its own encryption key and encryption/decryption algorithm. The communicating entities need not know or be able to perform the encryption algorithm of any of the other communicating entities.

Generally, in this embodiment each mobile station Mx is assigned an encryption key Emx and a decryption key Dmx. Dmx is known only at mobile station x. Each base station Bx of system 100 is assigned an encryption key Ebx and a decryption key Dbx. Dbx is known only at base station Bx. For any pair of mobile and base stations Mx and Bx desiring to communicate with each other, DmxEmx must equal EbxDmx.

When user of M1 desires to send a secure communication c to a user of M2, the communication c is encrypted by M1 using Em1 and Am1 to generate a message Em1(c). M1 then sends Em1(c) to base station B1 of the system. The base station B1 then encrypts Em1(c) using Eb1 and Ab1 to generate the message Eb1(Em1(c)) and sends it back to M1. M1 next decrypts Eb1(Em1(c)) using Dm1 and A1. Since  $Dm1Eb1=Db1Em1$ , decrypting Eb1(Em1(c)) using Dm1 and A2 results in Eb1(c). M1 then sends Eb1(c) to B1. M1 can be the only user who sends the correct Eb1(c) to B1 at this point. B1 now decrypts Eb1(c) using Db1 and Ab1 to generate c. B1 next sends c through the system to base station B2 that controls the area where user M2 is located. The communication c between B2 and M2 may then be encrypted in an identical manner to that described for the transfer between M1 and B1, with B2, Eb2, Db2 and Ab2, in place of M1, Em1, Dm1 and Am1, and, M2, Em2, Dm2 and Am2, in place of B1, Eb1, Db1 and Ab1.

Referring now to FIG. 3, therein is illustrated a flow diagram showing process steps performed to provide non-point to point encrypted communications within a telecommunications system according to an embodiment of the invention. The flow diagram of FIG. 3 can be used to describe an illustrative example, describing the case of a encrypted message transfer between mobile station M1 and mobile station M2 of FIG. 1. In this example, M1 and M2 use the Rabin algorithm and B1 and B2 use the RSA algorithm. The process used in FIG. 3 prevents mobiles M1 and M2 from having to perform the RSA algorithm used by the base stations.

The key functions Emy, Dmy, for mobile station My may be chosen according to the Rabin criteria. In the Rabin algorithm for this example, two prime numbers p and q are chosen using a selected number N, where  $p \times q = N$ , and  $p = 4k_1 + 3$ , and,  $q = 4k_2 + 3$ , and where  $k_1$  and  $k_2$  are constants.

N may be publicly known, and p and q must be kept private. Emy is defined as  $Emx(c)=(c)^2 \bmod N$  and, DMy is defined as  $DMy(c)=c^{1/2} \bmod N$ . To solve DMy(c) for c, the equations  $x^2=c \bmod p$ , and,  $x^2=c \bmod q$ , are solved using the solutions,  $x_1=\pm c^{(p+1)/4}$ , and,  $x_2=\pm c^{(q+1)/4}$ . If two values a and b are found such that  $ap+bq=1$ , then c can be found by the equation  $c^{1/2}=bqx_1+apx_2 \bmod N$ .

The key functions Ebx and Dbx for base station x may be chosen according to the Rivest, Shamir and Adleman(RSA) criteria. In RSA two (large) prime numbers p and q are first selected, where  $p \times q = N$ . Two other values, ax and bx, are then chosen, where  $(ax)(bx) = 1 \bmod (p-1)(q-1)$ . Ebx and Dbx are then defined as  $Ebx(c)=(c)^{ax} \bmod N$ , and,  $Dbx(c)=(c)^{bx} \bmod N$ . In this embodiment, N for B1 equals the N used for M1 and, N for B2 equals the N used for M2. This simplifies meeting the condition that  $Dm1Eb1=Eb1Dm1$ . However other values of N could be used as long as  $Dm1Eb1=Eb1Dm1$  and,  $Dm2Eb2=Eb2Dm2$ .

The process starts at step 300 where the encryption process is initiated. Next at step 302, communication c is encrypted at logic unit 112 of M1 using Em1 and Am1, to generate the encrypted message  $Em1(c)=(c)^2 \bmod N$ . The process then moves to step 304 where Em1(c) is transmitted through transceiver unit 104 from M1 to B1. At step 306, after receiving Em1(c) through transceiver unit 136, B1 encrypts Em1(c) using Eb1 and Ab1, to generate the encrypted message  $Eb1(Em1(c))=((c)^2)^{a1} \bmod N$ . The process then moves to step 308 where  $Em2(Em1(c))$  is sent back through transceiver unit 136 to M1 from B1. Next, at step 310, after receiving  $Em2(Em1(c))$  from B1 through transceiver unit 104, logic unit 112 of M1 decrypts Eb2(Em1(c)) using Dm1 and Rabin's algorithm, as described before.  $(Eb2(Em1(c)))^{1/2}=(((c)^2)^{a2})^{1/2}$ . The generated message  $Dm1(Eb2(Em1(c)))$  then equals  $(c)^{a2} \bmod N$ , or the encrypted message Eb2(c).

Next, at step 312, M1 sends the encrypted message Eb1(c) is sent to B1 through transceiver unit 104 and, at step 314 processor unit 140 of B1 then decrypts Eb1(c) using Db1 to generate  $Db1(Eb1(c))=((c)^{a1})^{b1} \bmod N=c$ . After the communication c is decrypted at processor 140 B1 the process moves to step 316 where the communication c is sent from control unit 138 of base station B1 through landline network 142 to control unit 130 base station B2. The transmission of communication c between B2 and M2 may then be performed in an identical manner to that described for the transfer between M1 and B1. This is illustrated by steps 318-330, which are identical to steps 302-314 with B2, Eb2, Db2 and Ab2, in place of M1, Em1, Dm1 and Am1, and, M2, Em2, Dm2 and Am2, in place of B1, Eb1, Db1 and Ab1.

The teachings of this invention should not be construed to be limited for use only with the telecommunications standards described, and should be construed to include any similar systems. Furthermore, other encryption algorithms than those expressly disclosed above may be employed to practice this invention.

Thus, the invention has been particularly shown and described with respect to preferred embodiments thereof, and it will be understood by those skilled in the art that changes in form and details may be made without departing from the spirit and scope of the invention.

What is claimed is:

1. In a telecommunications system having at least one base station and a plurality of mobile stations, a method for sending a secure message, said method comprising the steps of:

assigning each mobile station a decryption key and an encryption key, wherein each encryption key is public;

## 11

encrypting a first message at a first mobile station using the encryption key of said first mobile station to generate a second message;  
 transmitting said second message from said first mobile station to said at least one base station;  
 encrypting said second message at said at least one base station, using the encryption key of a second mobile station, to generate a third message;  
 transmitting said third message from said at least one base station to said first mobile station;  
 decrypting said third message at said first mobile station, using the decryption key of said first mobile station, to generate a fourth message;  
 transmitting said fourth message from said first mobile station to said at least one base station;  
 transmitting said fourth message from said at least one base station to said second mobile station; and  
 decrypting said fourth message at said second mobile station using the decryption key of said second mobile station to regenerate said first message.

2. The method of claim 1, wherein the decryption key and encryption key of said first mobile station and the decryption key and encryption key of said second mobile station are configured so that applying the encryption key of said second mobile station to a communication to obtain a first result, and then applying the decryption key of said first mobile station to the first result to obtain a final result, are equivalent in effect to applying the decryption key of said first mobile station to said communication to obtain a second result, and then applying the encryption key of said second mobile station to said second result to obtain said final result.

3. The method of claim 1, wherein said steps of encrypting and decrypting at said first mobile station are performed according to a first algorithm, and said steps of encrypting at said base station and decrypting at said second mobile station are performed according to a second algorithm.

4. The method of claim 3, wherein said first algorithm comprises an RSA type algorithm and said second algorithm comprises a Rabin type algorithm.

5. The method of claim 3, wherein said first algorithm comprises an Rabin type algorithm and said second algorithm comprises an RSA type algorithm.

6. In a telecommunications system, an apparatus for sending a secure message, said apparatus comprising:

a first mobile station, assigned a first decryption key and a first encryption key, said first mobile station for

## 12

encrypting a first message using said first encryption key to generate a second message, transmitting the second message on an air interface, receiving a third message on said air interface, decrypting the third message using said first decryption key to generate a fourth message, and transmitting the fourth message on said air interface;

a base station, said base station for receiving the second message on said air interface, encrypting the second message using a second encryption key to generate the third message, transmitting the third message on said air interface to said first mobile station, receiving the fourth message on said air interface from said first mobile station, and transmitting a fifth message on said air interface, wherein the fifth message includes the fourth message; and

a second mobile station, assigned a second decryption key and said second encryption key, said second mobile station for receiving the fifth message on said air interface from said base station and decrypting the fourth message included in the fifth message, using said second decryption key.

7. The apparatus of claim 6, wherein said first encryption key and said first decryption key and said second encryption key and said second decryption key are configured so that applying said second encryption key to a communication to obtain a first result, and then applying said first decryption key to the first result to obtain a final result are equivalent in effect to applying said first decryption key to said communication to obtain a second result, and then applying said second encryption key to said second result to obtain said final result.

8. The apparatus of claim 7, wherein encrypting and decrypting at said first mobile station are performed according to a first algorithm, and encrypting at said base station and decrypting at said second mobile station are performed according to a second algorithm.

9. The apparatus of claim 8, wherein said first algorithm comprises an RSA-type algorithm and said second algorithm comprises a Rabin-type algorithm.

10. The apparatus of claim 8, wherein said first algorithm comprises a Rabin-type algorithm and said second algorithm comprises an RSA-type algorithm.

\* \* \* \* \*

UNITED STATES PATENT AND TRADEMARK OFFICE  
**CERTIFICATE OF CORRECTION**

PATENT NO. : 5,909,491

DATED : June 1, 1999

INVENTOR(S) : Tie Luo

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 11, line 36, after "said" insert --at least one--.

Column 12, line 9, delete "a" and insert --at least one--.

Column 12, line 9, after "said" insert --at least one--.

Column 12, line 21, after "said" insert --at least one--.

Column 12, line 35, change "7" to --6--.

Column 12, line 37, after "said" insert --at least one--.

Signed and Sealed this

Fourteenth Day of September, 1999

Attest:



Q. TODD DICKINSON

Attesting Officer

Acting Commissioner of Patents and Trademarks